Please amend page 29, first full paragraph, to read as follows:

It should be understood that other quality of service issues may be factored into the above-identified scheme to allow the server to modify the value [M] N. In addition, other criteria similar to those set forth above[,] are contemplated and could be employed as part of the present invention.

AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the captioned Application:

Listing Of Claims:

Claim 1 (currently amended): A method for authenticating transferred data between a sender computer and a receiver computer over an open network comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

transmitting at least one token from the sender computer to the receiver computer during the first secure transmission, the number of tokens being set to a variable N;

establishing at least one additional transmission of data between the

sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission; [and]

comparing the at least one token transmitted from the sender computer during the at least one additional transmission to the at least one token transmitted from the sender computer during the first secure transmission to determine whether the transmission is authentic; and

each time a first secure transmission is performed, the sender computer transmits to the receiver computer a selected value of N and N number of tokens to be used to authenticate the sender computer.

Claim 2 (currently amended): The method [according to] set forth in claim 1, wherein the at least one token comprises a preselected number of tokens.

Claim 3 (currently amended): The method [according to] set forth in claim 2, wherein the number of at least one transmissions corresponds to the preselected number of tokens.

Claim 4 (currently amended): The method [according to] set forth in claim 2, wherein the number of at least one transmissions is greater [then] than the preselected number of tokens.

Claim 5 (currently amended): The method [according to] set forth in claim 2, wherein the number of at least one transmissions is less than the preselected number of tokens.

Claim 6 (currently amended): The method [according to] set forth in claim 1, wherein the at least one additional transmission is conducted over an unsecure or open connection.

Claim 7 (currently amended): The method [according to] set forth in claim 1, wherein the first secure transmission is encrypted.

Claim 8 (currently amended): The method [according to] set forth in claim 1, wherein the at least one additional transmission is sent in plaintext.

Claim 9 (currently amended): The method [according to] set forth in claim 5, wherein the at least one additional transmission is sent in plaintext.

Claim 10 (currently amended): The method [according to] set forth in claim 2, wherein the first secure transmission is encrypted.

Claim 11 (currently amended): The method [according to] set forth in claim 3, wherein the at least one additional transmission is sent in plaintext.

Claim 12 (currently amended): The method [according to] set forth in claim 1, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver verify that the checksum value is accurate by comparing the transmitted value to a checksum value generated using a similar checksum algorithm.

Claim 13 (currently amended): The method [according to] set forth in claim 10, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions.

Claim 14 (currently amended): A method for securely transferring data between a [sender] client computer and a [receiver] server over an open network comprising the steps of:

establishing a first secure transmission between the client computer and the server which is encrypted;

transmitting a preselected number of tokens from the client computer to the server during the first secure transmission, the number of tokens being set to a variable N;

establishing [a number of] additional transmissions between the client computer and the server corresponding to the preselected number of tokens N;

transmitting the data and one of the preselected tokens from the client computer during each additional transmission;

comparing the [transmitted] token transmitted during the additional transmis-

sion to the corresponding token transmitted during the first secure transmission; and

each time a first secure transmission is performed, the client computer transmits to the server a selected value of N and N number of tokens to be used to authenticate the client computer.

Claim 15 (currently amended): The method [according to] set forth in claim 14, wherein the additional transmissions are sent in plaintext.

Claim 16 (currently amended): The method [according to] set forth in claim 14, further comprising the steps of transmitting a checksum value during the first transmission and having the receiver computer verify that the checksum value is accurate by comparing the transmitted checksum value to a checksum value generated using a similar algorithm.

Claim 17 (currently amended): The method [according to] set forth in claim 16, wherein the transmitted checksum value is based upon checksum values transmitted during previous transmissions during this transaction.

Claim 18 (cancelled).

Claim 19 (currently amended): The method [according to] set forth in claim 1[8], wherein the [number of] additional transmissions [is] are variable and adaptively selected, at least in part, based upon the performance overhead of the system.

Claim 20 (currently amended): The method [according to] set forth in claim 1[8], wherein the [number of] additional transmissions [is] are variable and adaptively selected, at least in part, based upon monitored conditions.

Claim 21 (cancelled).

Claim 22 (currently amended): The method [according to] set forth in claim 2[2]3, wherein the algorithm is a statistical averaging algorithm.

On page 35, after paragraph 3, please add the following new claim:

- - 23. A method for authenticating transferred data between a sender computer and a receiver computer over an open network comprising the steps of:

establishing a first secure transmission of data between the sender computer and the receiver computer;

transmitting at least one token from the sender computer to the receiver computer during the first secure transmission, the number of tokens being set to a variable N;

establishing at least one additional transmission of data between the sender computer and the receiver computer;

transmitting the data and the at least one token from the sender computer to the receiver computer during the at least one additional transmission;